STANDARD: MOBILE DEVICES

Contents

1 Purpose

This standard specifies the technical requirements related to mobile devices that utilize the infrastructure and access Sensitive or Protected St. Lawrence University data.

2 Scope

St. Lawrence University considers mobile devices to be smart phones, tablets, or other types of highly mobile devices. Laptops are specifically excluded from the scope due to significant differences in security control options. There are two general types of mobile device categories that will impact the applicability of the Standard – University owned and BYOD (Bring Your Own Device)/personal devices.

Users include any mobile device that is able to connect and make use of the University's sensitive or protected information assets that include, but is not limited to all employees, faculty members, students, contractors, consultants, and approved guests.

3 Standard

3.1 Lost or Stolen devices

Contact the IT Help Desk (315.229.5770) and University Safety & Security (315.229.5555) if a device is lost or stolen.

3.2 Administration of Mobile Devices

Users of BYOD and university owned devices are responsible for the administration of the devices that they utilize.

The IT department will implement the ability to manage university owned devices as the technology is developed and deployed in our institutional infrastructure.

3.3 Remote Device Wipe

Users of BYOD and university owned devices are responsible for ensuring that remote wipe of their device is enabled.

Remote wipe of specific university protected and sensitive information will be deployed as the technology becomes available.

3.4 "Jailbroken", "Rooted", etc. Devices

Devices that have been modified to bypass security, sideload applications, and/or provide privileged control are prohibited.

3.5 Device Access Security

All devices must enable security measures (PIN, passcode, Biometrics, etc.) that protected the device from unauthorized used.

3.6 Encryption

All protected and sensitive data assets accessed on the mobile device must be encrypted. Refer to the St. Lawrence University Data Classification Policy.

3.7 Vulnerability Management

Mobile devices must be maintained with the most recent versions of operating system and software/apps as available from carriers, manufacturers, or software vendors.

IT will deploy patches and updates to University owned devices as the technology is developed and deployed in our infrastructure.

3.8 Compliance with State and Federal laws

Employees who use mobile devices to conduct University business must comply with all State and Federal laws related to those devices.

3.9 Camera-enabled devices

Capturing, recording, or transmitting images on a mobile device that may contain sensitive or protected university data is prohibited.

3.10 Ownership of University provided mobile devices

University provided mobile devices are institutional assets and are intended for business use.

All institution-provided mobile devices and associated telephone numbers are the property of St. Lawrence University.

Personal use of university provided mobile devices is not encouraged and use is restricted to the assigned employee with approval from their supervisor. Expenses associated with personal use are the responsibility of the assigned employee.

4 Standard review

This document will be reviewed on an annual basis and the results will be documented in the Revision History below. St. Lawrence University reserves the right to update this standard as necessary and all changes will be presented to the Information Technology Committee (ITC) for review.

Requests for changes to this policy may be made through the IT HelpDesk and will be directed to the appropriate group for review and inclusion as appropriate.

5 Related Standards, Policies and Processes

- St. Lawrence University Mobile Device Policy
- St. Lawrence University Acceptable Use Policy
- St. Lawrence University Data Classification Policy

6 Revision History

Version	Date	Author	Revisions/Reviews
d.02.00	2015-11-23	Sean Cunningham	Original
1.00.00	2015-12-18	Sean Cunningham	Updates, added content, updated comments from JS
1.00.01	2016-01-20	Sean Cunningham	Update – details from JR, RT, SM
1.00.02	2016-01-28	Sean Cunningham	Update – JS review
1.00.03	2016-02-03	Sean Cunningham	Standard review update based on ITC review.
1.00.04	2016-03-09	Sean Cunningham	Updates – JS review
1.00.04	2016-07-01	Sean Cunningham	Effective date

7 Approvals

VP for Library and Information Technology	Sponsor/Caretaker
Name	Name
Title	Title
Date	Date